View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA 69, 298–304 (1981)

Free Non-abelian Quotients of SL_2 Over Orders of Imaginary Quadratic Numberfields

FRITZ J. GRUNEWALD AND JOACHIM SCHWERMER

Sonderforschungsbereich "Theoretische Mathematik," Universität Bonn, Beringstr. 4, D-5300 Bonn 1, West Germany

Communicated by J. Tits

Received April 25, 1980

1. INTRODUCTION

Let $k = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic numberfield of discriminant $d < 0$, let R be an order of k. The main purpose of this paper is to prove that there exists a subgroup Γ of finite index of the special linear group $SL_2(R)$ of two-by-two matrices with determinant one and entries in R such that Γ has a free non-abelian quotient.

If R is the maximal order $\mathcal{O}_d$ of k a similar result was obtained by Zimmert [11] for certain discriminants d. He has proved that $SL_2(\mathcal{O}_d)$ has a free non-abelian quotient if a certain finite set associated to $\mathcal{O}_d$ has a cardinality greater than one. For a lot of small values of d his method does not work. Furthermore, it is not a priori clear that this condition is always satisfied for large values of d.

It is the aim of this note to indicate that a modification of the method of Zimmert can be used to give with some additional arguments a proof of our result.

As an immediate consequence one has that the groups $SL_2(R)$ for an order R of an imaginary quadratic numberfield are SQ-universal, this is, every countable group is isomorphic to a subgroup of a quotient of $SL_2(R)$. Whenever the maximal order $\mathcal{O}_d$ is an Euclidean domain, i.e., $d = -3, -4, -7, -8, -11$, Fine and Tretkoff [2] have proved this fact by a case-by-case study. In a concluding remark we observe that with respect to the property of SQ-universality the case $SL_2(\mathcal{O}_d)$ is an exceptional one in the framework of arithmetic groups.

0021-8693/81/040298-07\$02.00/0
Copyright © 1981 by Academic Press, Inc.
All rights of reproduction in any form reserved.

2. The Main Result

2.1. Theorem. *Let $k = \mathbf{Q}(\sqrt{d})$ be an imaginary quadratic numberfield of discriminant $d < 0$, let R be an order of k. Then there exists a subgrouup Γ of finite index of $SL_2(R)$ such that Γ has a free non-abelian quotient.*

Proof. Denote by $\mathcal{O}_d$ the ring of integers of k, i.e., the maximal order of k. Since each order of k is completely determined by its index in $\mathcal{O}_d$, we will write $R_d(m)$ for the order of index m. If 1, ω is a $\mathbf{Z}$-basis for $\mathcal{O}_d$, where $\omega = 1/2(\sqrt{d})$ if $d \equiv 0 \bmod 4$ resp. $\omega = 1/2(1+\sqrt{d})$ if $d \equiv 1 \bmod 4$ the order $R_d(m)$ has 1, $m\omega$ as a $\mathbf{Z}$-basis. For brevity we will use the notation $\Gamma_d = SL_2(\mathcal{O}_d)$ resp. $\Gamma_d(m) = SL_2(R_d(m))$ for the group of two-by-two matrices with determinant one and entries in $\mathcal{O}_d$ resp. $R_d(m)$.

We define with respect to the order $R_d(m)$ the set $W(m)$ as the set of natural numbers n which satisfy the following conditions:

(1) $4n^2 \leqslant m^2\,|\,d\,| - 3$,

(2) d is a quadratic non-residue modulo all the odd prime divisors of n, and if $d \not\equiv 5 \bmod 8$ n is odd,

(3) $n > 0$, $(n, m) = 1$ and $n \neq 2$.

It can happen that $W(m)$ is empty.

As the first step we prove the statement:

(*) *If the cardinality $w(m)$ of the set $W(m)$ associated to the order $R_d(m)$ is greater than one the group $\Gamma_d(m)$ has a free non-abelian quotient.*

The arguments given here for this fact are modifications for our purpose of the method of Zimmert [11], which are also indicated implicitly in [3]. So we only sketch the proof which goes along topological lines.

The group $SL_2(\mathbf{C})$ operates on the associated three-dimensional hyperbolic space H realized as

$$H = \{(z, r) \in \mathbf{C} \times \mathbf{R} \mid r > 0\}$$

by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}(z, r) = \left(\frac{(\bar{\delta} - \bar{\gamma}\bar{z})(\alpha z - \beta) - r^2\bar{\gamma}\alpha}{|\gamma z - \delta|^2 + r^2|\gamma|^2}, \frac{r}{|\gamma z - \delta|^2 + r^2|\gamma|^2}\right). \tag{4}$$

For further details we refer to [10, § 3]. We put $B := \{(z, r) \in H \mid |\gamma z - \delta|^2 + r^2|\gamma|^2 \geqslant 1$ for all γ, $\delta \in R_d(m)$ with $(\delta, \gamma) = 1\}$. For each $n \in W(m)$ and $t \in \mathbf{Z}$ with $(n, t) = 1$ we define $F_{n,t} := B \cap \{(z, r) \in H \mid \operatorname{Im}(z - (t/n)\ \ m\omega) \leqslant (m^4|d|^2)^{-1}\}$, where $\operatorname{Im}(\ )$ denotes the imaginary part of a complex number. Condition (1) implies that the sets $F_{n,t}$

are disjoint for distinct pairs $\langle n, t\rangle$. Using these strips we define for each $n \in W(m)$ a map

$$e_n : B \to S^1 = \{z \in \mathbf{C} \,|\, |z| = 1\}$$

by

$$e_n((z, r)) = \begin{cases} 1 & \text{if} \quad (z, r) \notin \bigcup\limits_{\substack{t \\ (n,t)=1}} F_{n,t} \\ \exp 2\pi i \left(\dfrac{1}{2} + \dfrac{m^4 |d|^2}{2} \operatorname{Im}\left(z - \dfrac{t}{n} m\omega\right)\right) & \text{if} \quad (z, r) \in F_{n,t}. \end{cases}$$

The natural projection $B \to \Gamma_d(m)\backslash H$ is surjective, and a word-for-word generalization of Hilfssatz 1 in [11] shows that we have a unique factorization of e_n over $\Gamma_d(m)\backslash H$ by a continuous map

$$f_n : \Gamma_d(m)\backslash H \to S^1. \tag{5}$$

Define Y as the one-point-union of $w(m)$ copies of the sphere S^1 taking as base-point the point 1. The inclusion $Y \to \Pi S^1$ induces an isomorphism $H_1(Y; \mathbf{Z}) \cong \Pi H_1(S^1; \mathbf{Z})$ of the homology with integer coefficients. Patching the continuous maps f_n together we get a continuous map

$$f : \Gamma_d(m)\backslash H \to Y, \tag{6}$$

which can be viewed by an appropriate choice of a base point h in $\Gamma_d(m)\backslash H$ as a map of pointed spaces. Therefore f induces a homomorphism

$$f_* : \pi_1(\Gamma_d(m)\backslash H, h) \to \pi_1(Y, 1) \tag{7}$$

on the level of the fundamental group. We remark that $\Gamma_d(m)\backslash H$ is path-wise connected.

To each $g \in \Gamma_d(m)$ we associate now the class in $\pi_1(\Gamma_d(m)\backslash H, h)$ which is given by the image in $\Gamma_d(m)\backslash H$ of a path from h to $g \cdot h$ in H. This defines a homomorphism

$$\phi : \Gamma_d(m) \to \pi_1(\Gamma_d(m)\backslash H, h). \tag{8}$$

If we combine now the homomorphism ϕ with f_* we get the homomorphisms

$$F : \Gamma_d(m) \to \pi_1(Y, 1) \tag{9}$$

resp.

$${}_HF : \Gamma_d(m) \to H_1(Y; \mathbf{Z}) \tag{10}$$

defined by $F = f_* \circ \phi$ resp. ${}_H F = H \circ F$ where H denotes the Hurewicz-homomorphism.

Now we will show that ${}_H F$ is surjective. Once we have proved this we are through. The group $F(\Gamma_d(m))$ is as a subgroup of the free non-abelian group $\pi_1(Y, 1)$ a free group. The quotient $H_1(Y; \mathbf{Z})$ of $F(\Gamma_d(m))$ is a free abelian group of rank $w(m)$. Therefore $F(\Gamma_d(m))$ is a free non-abelian group of at least $w(m)$ generators.

By taking the path $x \mapsto \exp 2\pi i x$ as a generator for $H_1(S^1; \mathbf{Z})$ we identify $H_1(S^1; \mathbf{Z})$ with $\mathbf{Z}$. Let g be an element of $\Gamma_d(m)$ such that there exist (z, r), $(z', r') \in B$ with $g \cdot (z, r) = (z', r')$. Then the value $F_n(g)$ of $F_n : \Gamma_d(m) \to H_1(S^1; \mathbf{Z}) \cong \mathbf{Z}$ which is defined in the same way as F is given by (cf. [11])

$$F_n(g) = \operatorname{card} \left\{ k \in \mathbf{Z} \;\middle|\; \operatorname{Im} z < \operatorname{Im} \frac{k}{n} m\omega \leqslant \operatorname{Im} z', \ (n, k) = 1 \right\}$$
$$\text{if } \operatorname{Im} z \leqslant \operatorname{Im} z', \tag{11}$$

resp.

$$F_n(g) = -\operatorname{card} \left\{ k \in \mathbf{Z} \;\middle|\; \operatorname{Im} z' < \operatorname{Im} \frac{k}{n} m\omega \leqslant \operatorname{Im} z, \ (n, k) = 1 \right\}$$
$$\text{if } \operatorname{Im} z' < \operatorname{Im} z. \tag{12}$$

This gives us a hint how to construct appropriate elements in $\Gamma_d(m)$ whose image under $\prod F_n$ span $\prod H_1(S^1; \mathbf{Z})$.

We imitate the construction given in [11]. The elements of $W(m)$ are indexed in such a way that

$$\frac{r_1}{n_1} > \frac{r_2}{n_2} > \cdots > \frac{r_{w(m)}}{n_{w(m)}},$$

if r_i denotes the greatest natural number which is smaller than $n_i/2$ and satisfies $(n_i, r_i) = 1$. The congruences

$$-|a_i + m\omega|^2 \equiv |b_i + m\omega|^2 \bmod n_i \tag{13}$$

are solvable in a_i and b_i, $i = 1, \ldots, w(m)$, since in a finite field every element is the sum of two squares. Now condition (2) in the definition of $W(m)$ implies $(|a + m\omega|^2, n_i) = 1$ for all $a \in \mathbf{Z}$ and $i = 1, \ldots, w(m)$. Therefore we can find integers $s_i \in \mathbf{Z}$ which satisfy the conditions

$$\begin{aligned} r_i s_i |a_i + m\omega|^2 &\equiv 1 \bmod n_i \\ -r_i s_i |b_i + m\omega|^2 &\equiv 1 \bmod n_i \\ n_i - r_i < s_i \qquad &\text{for} \quad i = 1, \ldots, w(m). \end{aligned} \tag{14}$$

Put

$$\sigma_i = \begin{pmatrix} s_i\overline{(a_i + m\omega)} & * \\ n_i & r_i(a_i + m\omega) \end{pmatrix},$$

$$\tau_i = \begin{pmatrix} (n_i - r_i)\overline{(b_i + m\omega)} & * \\ n_i & s_i(b_i + m\omega) \end{pmatrix}$$

where $^-$ denotes complex conjugation as usual. Define $z_i = r_i(a_i + m\omega)/n_i$, $v_i = s_i(b_i + m\omega)/n_i$ and $t_i = 1/n_i$ for $i = 1,\ldots, w(m)$. Then one gets

$$\sigma_i(z_i, t_i) = (z_i', t_i) \qquad \text{resp.} \quad \tau_i(v_i, t_i) = (v_i', t_i) \tag{15}$$

where $z_i' = -s_i\overline{(a_i + m\omega)}/n_i$, $v_i' = -(n_i - r_i)\overline{(b_i + m\omega)}/n_i$. Just as in Hilfssatz 1 in [11] one shows that (z_i, t_i), (z_i', t_i), (v_i, t_i), $(v_i', t_i) \in B$ for all $i = 1,\ldots, w(m)$. Define $\gamma_i := \tau_i \sigma_i$ for $i = 1,\ldots, w(m)$. Then formulas (11), (12) imply

$$F_{n_j}(\gamma_i) = 0 \qquad \text{for} \quad j < i \qquad \text{and} \quad F_{n_j}(\gamma_j) = 1. \tag{16}$$

It follows that $\prod_{n \in W(m)} F_n$ is surjective; this yields the desired surjectivity of ${}_H F$.

This completes the proof of statement $(*)$.

Now we consider the group $\Gamma_d(m)$ for a given order $R_d(m)$ in k. If $w(m) > 1$ we are through by statement $(*)$. So assume $w(m) \leqslant 1$. By an old result about primes in quadratic numberfields (cf. Satz 147 in [4]) it follows that there exist an infinite number of odd primes p such that d is a quadratic non-residue modulo p. Therefore one can find three odd prime numbers p_1, p_2, p_3 satisfying

$$p_1 < p_2 < p_3, \tag{17}$$

$$(p_i, m) = 1 \qquad \text{for} \quad i = 1,\ 2,\ 3, \tag{18}$$

$$d \text{ is a quadratic non-residue modulo } p_1, \text{ i.e., } (d/p_1) = -1. \tag{19}$$

Put $m' := m \cdot p_2 \cdot p_3$; then it is easy to verify that one has $p_1 \in W(m')$. An iteration of this construction implies that one can find an order $R_d(q)$ with m dividing q and $w(q) > 1$. Now $\Gamma_d(q)$ is of finite index in $\Gamma_d(m)$ and has a free non-abelian quotient.

3. A Remark on the SQ-Universality for Arithmetic Groups

Theorem 2.1 implies that the groups $SL_2(R)$ for an order R of an imaginary quadratic numberfield are SQ-universal, i.e., every countable group is isomorphic to a subgroup of a quotient of $SL_2(R)$. This fact exhibits with respect to this property the case $SL_2(R)$ as an exceptional one in the framework of arithmetic groups.

3.1. THEOREM. *Let K be an algebraic numberfield and R an order of K. Then the group $SL_n(R)$ is SQ-universal if and only if $n = 2$ and either $K = \mathbf{Q}$ or K is an imaginary quadratic numberfield.*

Observing the lemma in [8] this follows from Theorem 2.1, the well-known fact that the group $SL_2(\mathbf{Z})$ is SQ-universal [8] and the following theorem due to Margulis which is implicitly contained in his results in [5–7]. Since it is not formulated there, we give it explicitly.

Let V denote the set of primes (or of equivalence classes of absolute values) of K; denote by V_∞ the set of infinite primes of K. For $v \in V$, let K_v denote the completion of K with respect to v. If G is a linear algebraic group defined over K, we denote by $G(K)$ the group of K-rational points of G. (For details on algebraic and arithmetic groups see [1]).

3.2. THEOREM (Margulis). *Let G be a connected semisimple almost K-simple linear algebraic group defined over K. Assume that G satisfies the following condition*

$$\sum_{v \in V_\infty} rk_{K_v}(G) \geqslant 2 \qquad \text{(M)}$$

where $rk_{K_v}(G)$ denotes the K_v-rank of G. Then, if N is a normal subgroup of an arithmetic subgroup Γ of $G(K)$, either Γ/N is finite or N is central in $G(K)$.

Using the result that Γ is finitely generated (cf. [1, § 12]) one deduces from Margulis' theorem that Γ has only countably many non-isomorphic normal subgroups. Since a countable group which is SQ-universal has $2^{\aleph_0}$ non-isomorphic factor groups (cf. [8, § 3]) we get

3.2. COROLLARY. *Let G be a connected semisimple almost K-simple linear algebraic group defined over K which satisfies the condition* (M). *Then no arithmetic subgroup Γ of $G(K)$ is SQ-universal.*

REFERENCES

1. A. BOREL AND HARISH-CHANDRA, Arithmetic subgroups of algebraic groups, *Ann. of Math.* **75** (1962), 485–535.
2. B. FINE AND M. TRETKOFF, The SQ-universality of certain arithmetically defined linear groups, *J. London Math. Soc.* **13** (1976), 65–68.
3. F. GRUNEWALD, H. HELLING, AND J. MENNICKE, SL_2 over complex quadratic number fields, *Algebra i Logica* **17** (1978), 512–580.

4. E. HECKE, "Vorlesungen über die Theorie der algebraischen Zahlen," Leipzig, 1923 (Reprint New York, 1970).
5. G. A. MARGULIS, Quotient groups of discrete subgroups and measure theory, *Funkts. Anal. Prilozhen.* **12**, No. 4 (1978), 64–80.
6. G. A. MARGULIS, Finiteness of factor groups of discrete subgroups, *Funkts. Anal. Prilozhen.* **13**, No. 3 (1979), 178–187.
7. G. A. MARGULIS, Factor groups of discrete subgroups, *Dokl. Akad. Nauk. SSSR.* **242**, No. 3, (1979), 533–536.
8. P. M. NEUMANN, The SQ-universality of some finitely presented groups, *J. Austral. Math. Soc.* **16** (1973), 1–6.
9. M. S. RANGHUNATHAN, On the congruence subgroup problem, *Publ. Math. IHES* **46** (1976), 107–162.
10. R. SWAN, Generators and relations for certain special linear groups, *Advances in Math.* **6** (1971), 1–77.
11. R. ZIMMERT, Zur SL_2 der ganzen Zahlen eines imaginär-quadratischen Zahlkörpers, *Invent. Math.* **19** (1973), 73–82.